When Tomorrow Becomes Today

As a child, I watched *The Jetsons*; it was a great show that I thoroughly enjoyed, but it led me to picture a 21st century where we would all be teleporting or driving personal spacecrafts to work. Likewise, my envisioned work environment included robots, mobile phones, and automated food mechanisms arriving at my desk at timely intervals throughout the day to provide hot and delicious snacks—all of this located within my organization where we manufactured fabulous cosmic products.

Looking back, if you trade my Toyota 4Runner for the spacecraft, my imagination was amazingly accurate. Allow me to compare my anticipated workplace with reality: Currently, my organization is heavily involved in robotics for use in various arenas; my cell phone can connect to anywhere in the world and can tell me where in the world I am; we produce software for use in all five levels of the Earth's atmosphere and outer space; and, for a few coins, I can eat food served to me from a vending machine—all of these are great advancements. Okay, the vending machine is a bit of a stretch, as at-work food delivery, or the quality of the snacks, hasn't evolved much. I guess we still have frontiers to be explored—at least gastronomically, if not astronomically.

The November/December issue of CROSSTALK, themed *21st Century Defense*, explores slightly different advancements specific to the software defense industry. The software battlefront now includes laptops, desktops, servers, PDAs, cell phones, personal identification cards, and even a soldier's clothing. Each of these devices are utilized in our defense of the nation, as well as used against us by cyberattackers. Similarly, developing nations are advancing their technology at a more rapid pace than ever before. Electronic warfare (attack, support, and protection), drones, artificial intelligence, space platforms, miniature weaponry, and directed energy are all part of the new strategies planned in the defense of nations. Many of these weapons are nonlethal, but not all; many are aimed at rendering defense forces powerless by destroying software and systems before they can serve their purpose. The need to progress in our defense strategies and capabilities has never been greater, and this issue of CROSSTALK presents several ideas to forward the cause.

We begin with *The Combat-Wireless Health Monitoring System* by MAJ Phillip G. Burns, who shares advances in identifying and monitoring a soldier's health and assessing injuries during combat, in turn speeding traumatic care and saving lives. Next, Susan Chandler and Jerrod Loyless' *PKI: The DoD's Critical Supporting Infrastructure for Information Assurance* (IA) explores the effective use of public key cryptography and how the Air Force is employing this technology to improve IA. In our final themed article, Summer Olmstead and Dr. Ambareen Siraj discuss the definition, history, laws, and defense methodologies of the new battlefront in *Cyberterrorism: The Threat of Virtual Warfare*.

Also in this issue, Anthony David Scott, Michael Malloy, Peter Clay, and Mark Masone's article—*Certification and Accreditation of SOA Implementations: Programmatic Rules for the DoD*—provides some interesting and valuable guidance for those faced with rapidly changing requirements on an SOA project. Finally, don't miss Jim O'Brien's *Preparing for an Internal Assessment Interview*, which offers practical insights regarding the nature of assessors and assists organizations in successfully participating in and surviving their next assessment.

It is our hope that this issue of CROSSTALK will set the reader's mind in motion, stimulating new thoughts in regard to the future of software defense. There is no doubt that together, with the collective ideas and innovation of today, we will continue to be safe and secure well into the 22nd century.

Karl Rogers

Karl Rogers
Director, 309th Software Maintenance Group
Co-Sponsor